ELSEVIER

Discrete Mathematics 167/168 (1997) 167–174

DISCRETE MATHEMATICS

Strongly 2-perfect cycle systems and their quasigroups[1]

Darryn E. Bryant, Sheila Oates-Williams *

Centre for Combinatorics, Department of Mathematics, The University of Queensland, Qld 4072, Australia

Received 7 July 1995; revised 2 November 1995

Abstract

A recent result of Bryant and Lindner shows that the quasigroups arising from 2-perfect m-cycle systems form a variety only when $m = 3$, 5 and 7. Here we investigate the situation in the case where the distance two cycles are required to be in the original system.

1. Introduction

The idea of cycle systems and their associated groupoids seems to have appeared first in the work of Kotzig [6] and several authors have since worked with this concept ([8] gives an excellent survey). Additional structure of the decomposition of K_v into m-cycles may be required. One such property is that of being *i-perfect*. The case where $i = 2$ is of particular interest, because then, as was shown by Keedwell [4, 5], the associated groupoid is a quasigroup, which he called a *P-quasigroup*. The question as to when these form a variety has been intensively studied (see [7]). In their paper, Bryant and Lindner [2], showed that the quasigroups arising from 2-perfect m-cycle systems form a variety only for $m = 3$, 5 and 7. In [3], we looked at the question of finding additional laws which held in P-quasigroups of small order. In this paper we investigate whether varieties can be obtained by placing additional restrictions on the 2-perfect systems considered.

2. Definitions and preliminary results

Definition 2.1. An m-cycle system of order n is a decomposition of the complete graph K_n on n vertices into edge disjoint cycles of length m. It is *i-perfect* if every pair of vertices occurs at distance i in a unique cycle.

* Corresponding author. E-mail: sw@maths.uq.oz.au.

[1] This work was supported by grants from the Australian Research Council and the University of Queensland.

PII S0012-365X(96)00225-7

Given any cycle system, we can define a binary operation $\star$ on the vertices of the graph by defining $a \star b = c$ and $c \star b = a$ whenever $(\ldots, a, b, c, \ldots)$ is a cycle of the system and $a \star a = a$. The resulting groupoid is a quasigroup precisely when the system is 2-perfect. In order to write down the laws satisfied by these quasigroups, it is convenient to have some notation.

Definition 2.2 (Bryant [1]). Let $\star$ be a binary operation symbol. The sequence of words $W_i(x, y)$ is defined inductively by

$$W_0(x, y) = x, \tag{1}$$

$$W_1(x, y) = y, \tag{2}$$

$$W_i(x, y) = W_{i-2}(x, y) \star W_{i-1}(x, y). \tag{3}$$

An important consequence of this definition is

$$W_2(W_{i-2}(x, y), W_{i-1}(x, y)) = W_{i-2}(x, y) \star W_{i-1}(x, y) = W_i(x, y). \tag{4}$$

Lemma 2.3. *The quasigroups arising from a 2-perfect m-cycle system satisfy the laws*

$$W_2(x, x) = x, \tag{5}$$

$$W_2(W_2(x, y), y) = x, \tag{6}$$

$$W_m(x, y) = x, \tag{7}$$

$$W_{m+1}(x, y) = y. \tag{8}$$

A consequence of (4) and (5) is

$$W_i(x, x) = x, \tag{9}$$

and a consequence of (4) and (6) is

$$W_2(W_i(x, y), W_{i-1}(x, y)) = W_{i-2}(x, y). \tag{10}$$

Unfortunately, it is not true in general that quasigroups satisfying the laws of Lemma 2.3 give rise to m-cycle systems; as was shown by Bryant and Lindner [2], this happens in general only for $m = 3$, 5 and 7. The basic problem is that the 'cycle' $(W_0, W_1, \ldots, W_{m-1})$ may contain repetitions. In [3] we looked at methods of overcoming this problem in cycle systems of small order. Here we seek to solve it by imposing extra conditions on the cycle system.

Definition 2.4. A 2-perfect m-cycle system is said to be *strongly 2-perfect* if the distance two cycles also belong to the system. (Note that this implies that m must be odd, and from now on we shall assume this to be so.)

Example 2.5. Let p be an odd prime and let $\mathscr{B}$ be a balanced incomplete block design with parameters $v, b, r, p, 1$. On a given block $a_1, a_2, \ldots, a_p$ draw the complete

graph K_p and decompose this into the disjoint cycles $(a_1, a_2, a_3, \ldots a_p)$, $(a_1, a_3, a_5, \ldots, a_p, a_2, a_4, \ldots, a_{p-1}), \ldots, (a_1, a_{(p+1)/2}, a_p, \ldots, a_{(p+3)/2})$. The result is a strongly 2-perfect p-cycle system on the complete graph K_v.

In many cases, a strongly 2-perfect cycle system has to be of the type described in the previous example.

Lemma 2.6. *Let p be a prime such that either*

(a) 2 *has order* $p-1$ *modulo* p; *or*

(b) 2 *has order* $(p-1)/2$ *and* $p \equiv 3 \bmod 4$.

Then in any strongly 2-perfect cycle system, if p points lie on a cycle, then the iterated distance 2-cycles cover all of the edges between these points.

Proof. The conditions on p ensure that the process of iterating the construction of the distance 2-cycles yields all $(p-1)/2$ cycles on any p points which lie on a cycle. (The extra condition in case (b) implies that -1 is not a power of 2, so that all $(p-1)/2$ powers of 2 yield different cycles. For instance, with $m = 7$ we get the cycles at distances 1, 2 and 4 $(= -3)$, whereas, with $m = 17$, we get only the cycles at distances 1, 2, 4 and 8, because $16 = -1$, $32 = -2$, etc.)

Consider the variety generated by the quasigroups arising from all strongly 2-perfect m-cycle systems. This will satisfy the laws of Lemma 2.3, and so any finite member will give rise to a decomposition of a complete graph into closed trails, but there is no a priori reason why these should be cycles. For instance, with $m = 9$, we might get a trail of the form $a, b, c, a, d, e, f, g, h, a$. However, if we can prove from laws which are satisfied by quasigroups arising from all strongly 2-perfect m-cycle systems that $W_i(x, y) = W_j(x, y)$ for some i, j with $0 \leqslant i < j \leqslant m-1$ implies all W_r are equal, then no non-trivial closed trails which are not cycles can occur, so we shall have shown that the ONLY finite quasigroups which satisfy the laws are those corresponding to strongly 2-perfect m-cycle systems. This proves that these quasigroups are the finite quasigroups of the variety determined by the laws of Lemma 2.3. Clearly, the implication will be true if $W_i(x, y)$ and $W_j(x, y)$ are adjacent in a distance 2^k-cycle, for some k, by (3) and (5). Hence we seek to show that the equality of any of the W's implies that of two W's whose distance apart is a power of 2 in the original cycle. This happens automatically in the situations covered by Lemma 2.6. The following lemmata will be useful in our calculations.

Lemma 2.7. *If a groupoid satisfies the laws of Lemma* 2.3, *then, for all non-negative integers i, j.*

$$W_i(W_j(x, y), W_{j+1}(x, y)) = W_{i+j}(x, y). \tag{11}$$

Proof. This is [1, Lemma 2.2.2]: since this is not readily available, we give the proof here.

Let P_k be the proposition that for all integers j, $W_k(W_j, W_{j+1}) = W_{k+j}$ (omitting x and y to simplify the notation). We first prove by induction on k that P_k is true for all non-negative integers k. If $k = 0$, then

$$W_k(W_j, W_{j+1}) = W_0(W_j, W_{j+1}) = W_j \quad \text{by (1)}.$$

If $k = 1$, then

$$W_k(W_j, W_{j+1}) = W_1(W_j, W_{j+1}) = W_{j+1} \quad \text{by (2)}.$$

Thus, P_0 and P_1 are true. Now suppose $k \geqslant 1$ and P_i true for $0 \leqslant i \leqslant k$. Consider P_{k+1}.

$$\begin{aligned} W_{k+1}(W_j, W_{j+1}) &= W_{k-1}(W_j, W_{j+1}) \bigstar W_k(W_j, W_{j+1}) \quad \text{by (3)} \\ &= W_{k+j-1} \bigstar W_{k+j} \quad \text{by the induction hypothesis} \\ &= W_{k+1+j} \quad \text{by (3)}. \end{aligned}$$

Thus P_{k+1} is true, so P_k is true for all non-negative integers k. To extend the result to negative integers, we need to show that if P_k is true for all $i \geqslant k$, then P_{k-1} is true.

$$\begin{aligned} W_{k-1}(W_j, W_{j+1}) &= W_{k+1}(W_j, W_{j+1}) \bigstar W_k(W_j, W_{j+1}) \quad \text{by (10)} \\ &= W_{k+j+1} \bigstar W_{k+j} \quad \text{by the induction hypothesis} \\ &= W_{k-1+j} \quad \text{by (10)}. \end{aligned}$$

Hence P_{k-1} is true, so P_k is true for all integers k. □

Lemma 2.8. *If a groupoid $(G, \bigstar)$ which satisfies the laws of Lemma 2.3 also satisfies the law*

$$W_2(W_0(x, y), W_2(x, y)) = W_4(x, y), \tag{12}$$

then it satisfies the laws

$$W_i(W_j(x, y), W_{j+2^k}(x, y)) = W_{j+i2^k}(x, y), \quad (i, j \in \mathbb{Z},\ k \in \mathbb{N}_0). \tag{13}$$

Proof. Since (10) and (13) together imply that

$$W_2(W_4(x, y), W_2(x, y)) = W_0(x, y),$$

it is clearly sufficient to prove the result for $i, j, k \in \mathbb{N}_0$, the result for negative i and j then follows as in the previous lemma. We prove this in various stages. Again, to simplify the notation we shall omit (x, y).

Step 1: For all j,

$$W_2(W_j, W_{j+2}) = W_{j+4}. \tag{14}$$

We use the condition $W_2(W_0, W_2) = W_4$.

$$\begin{aligned} W_2(W_j, W_{j+2}) &= W_2(W_0(W_j, W_{j+1}), W_2(W_j, W_{j+1})) \quad \text{by (1) and (4)} \\ &= W_4(W_j, W_{j+1}) \quad \text{by (12)} \\ &= W_{j+4} \quad \text{by (11).} \end{aligned}$$

Step 2: For all i, j,

$$W_i(W_j, W_{j+2}) = W_{j+2i}. \tag{15}$$

We prove this by induction on i. It is true for $i = 0, 1, 2$, by (1), (2) and (14), so suppose $i > 2$ and result true for all ℓ, $0 \leqslant \ell < i$ and consider i.

$$\begin{aligned} W_i(W_j, W_{j+2}) &= W_2(W_{i-2}(W_j, W_{j+2}), W_{i-1}(W_j, W_{j+2})) \quad \text{by (4)} \\ &= W_2(W_{j+2(i-2)}, W_{j+2(i-1)}) \quad \text{by the induction hypothesis} \\ &= W_{j+2i} \quad \text{by (14).} \end{aligned}$$

Hence, the result is true for all i.

Step 3: For all i, j, k,

$$W_i(W_j, W_{j+2^k}) = W_{j+i2^k}. \tag{16}$$

We prove this by induction on k. It is true for $k = 0, 1$, by (11) and (15), so suppose $k > 1$ and result true for $k - 1$ (and all i, j).

$$\begin{aligned} W_i(W_j, W_{j+2^k}) &= W_i(W_0(W_j, W_{j+2^{k-1}}), W_2(W_j, W_{j+2^{k-1}})) \quad \text{by (1) and (14)} \\ &= W_i(W_j, W_{j+2^{k-1}}) \quad \text{by the induction hypothesis} \\ &= W_{j+2i\times 2^{k-1}} \quad \text{by (15)} \\ &= W_{j+i2^k}. \end{aligned}$$

Hence, the result is true for all k.

Note that the last result shows that only one extra law is needed in order to ensure that a P-quasigroup corresponds to a strongly 2-perfect system. What this result tells us is that if $j - i = \pm 2^k$, $k \in \mathbb{N}_0$, then $(\ldots, W_i, W_j, W_{j+(j-i)}, \ldots)$ is in the system, and so the system is strongly 2-perfect. □

3. The quasigroups

The problem in recovering the cycle system from the quasigroup lies in ensuring that $(W_0, W_1, \ldots, W_{m-1})$ really is a cycle, i.e. that no coincidences occur. Thus, we want to show that a condition such as $W_0 = W_i$ causes the whole cycle to collapse. If $i = 2^k$ for some k, and $W_i = W_0$, we have $W_{2i} = W_0 \bigstar W_i = W_0$ and so on, so the cycle

does collapse. Also, if $i = 2^k r$ where r is odd, then W_0 and W_i are distance r apart in the 2^k-distance cycle. Finally, since if i is odd, $m - i$ is even, we need check only the cases where i is odd and does not exceed $(m-1)/2$. In fact, exploiting these two ideas, we have the following lemma.

Lemma 3.1. *Let m be an odd number and let $S = \{a \in \mathbb{N} \mid 0 < a \leqslant (m-1)/2, a \text{ odd}\}$. Define the map $\sigma : S \to S$ as follows. If $m - a = 2^k b$, where b is odd, then $a\sigma = b$. Then σ is a permutation of S.*

Proof. Since $a \geqslant 1$ and $k \geqslant 1$, σ does map S to S. It thus suffices to prove that σ is onto. But, given $b \in S$ there is a unique power 2^k such that $m/2 \leqslant 2^k b < m$. Set $a = m - 2^k b$, then $a\sigma = b$. □

As a consequence of this result, we need only check $W_0 = W_j$ for one j in each cycle of σ. In particular, there is no checking needed for the numbers in the cycle containing 1. Here are two more lemmata which assist in settling various cases.

Lemma 3.2. *If $W_0 = W_3$ and $3 \nmid m$, then $W_0 = W_r$ for $0 \leqslant r \leqslant m$.*

Proof. We prove by induction on r that $W_{3r+j} = W_j$ for $j = 0, 1, 2$. For $r = 1$ we already have $W_3 = W_0$. But $W_4 = W_0 \bigstar W_2 = W_3 \bigstar W_2 = W_1$ and $W_5 = W_3 \bigstar W_4 = W_0 \bigstar W_1 = W_2$. Hence, the result holds for $r = 1$. Now assume $r > 1$ and result true for $r-1$ and consider r. $W_{3r} = W_{3r-2} \bigstar W_{3r-1} = W_{3(r-1)+1} \bigstar W_{3(r-1)+2} = W_1 \bigstar W_2 = W_3 = W_0$, and similarly for W_{3r+1} and W_{3r+2}. Since $3 \nmid m$, it follows that $W_0 = W_m = W_1$ or W_{-1} so the cycle collapses. □

Lemma 3.3. (a) *If $W_0 = W_{2^k-1}$ then $W_{2^k+i} = W_{(i+1)2^k}$;*
(b) *If $W_0 = W_{2^k+1}$ then $W_{2^k-i} = W_{(i+1)2^k}$.*

Proof. (a) $W_{2^k+1} = W_{2^k-1} \bigstar W_{2^k} = W_0 \bigstar W_{2^k} = W_{2\times 2^k}$; $W_{2^k+2} = W_{2^k} \bigstar W_{2^k+1} = W_{2^k} \bigstar W_{2\times 2^k} = W_{3\times 2^k}$ and so on.

(b) $W_{2^k-1} = W_{2^k+1} \bigstar W_{2^k} = W_0 \bigstar W_{2^k} = W_{2\times 2^k}$. $W_{2^k-2} = W_{2^k} \bigstar W_{2^k-1} = W_{2^k} \bigstar W_{2\times 2^k} = W_{3\times 2^k}$ and so on.

4. The theorem

In this section we gather into one statement our current knowledge of the cases in which the quasigroups corresponding to strongly 2-perfect m-cycle systems do form a variety.

Theorem 4.1. *Let*
(a) *m be an odd prime less than* 127; *or*
(b) *m be a prime greater than* 127 *to which the conditions of Lemma* 2.6 *apply.*

Then the quasigroups corresponding to strongly 2-perfect m-cycle systems form a variety defined by the laws:

$$W_2(x,x) = x,$$

$$W_2(W_2(x,y),y) = x,$$

$$W_m(x,y) = x,$$

$$W_{m+1}(x,y) = y,$$

$$W_2(W_0(x,y),W_2(x,y)) = W_4(x,y).$$

Proof. By the remark following Lemma 2.6, we need only show that $W_0 = W_i$ $(1 \leqslant i \leqslant (m-1)/2)$ implies collapsing in any strongly 2-perfect m-cycle system,

Case (b) follows immediately from Lemma 2.6.

For (a), we note that the only cases not covered by Lemma 2.6 are 17, 31, 41, 43, 73, 89, 97, 109 and 113. We consider each of these in turn.

$m = 17$: Here $\sigma = (1)(3\,7\,5)$, so we check only $i = 3$ which is covered by Lemma 3.2.

$m = 31$: Here $\sigma = (1\,15)(3\,7)(5\,13\,9\,11)$, so we check $i = 3$ which is covered by Lemma 3.2., and $i = 5$. In the latter case, by Lemma 3.3(b) we have $W_1 = W_{16} = W_{-15}$. Since these are distance 16 apart, the cycle collapses.

$m = 41$: Here $\sigma = (1\,5\,9)(3\,19\,11\,15\,13\,7\,17)$, so we check only $i = 3$ which is covered by Lemma 3.2.

$m = 43$: Here $\sigma = (1\,21\,11)(3\,5\,19)(7\,9\,17\,13\,15\,7)$, so we check $i = 3$ which is covered by Lemma 3.2, and 7. For $i = 7$, by Lemma 3.3(a), we have $W_{13} = W_{48} = W_5$, so the cycle collapses.

$m = 73$: Here $\sigma = (1\,9)(3\,35\,19\,27\,23\,25)(5\,17\,7\,33)(11\,31\,21\,13\,15\,29)$, so we check $i = 3$ which is covered by Lemma 3.2, 5 and 15. For $i = 5$, by Lemma 3.3(b), we have $W_{-9} = W_{56} = W_{-17}$, so the cycle collapses and for $i = 15$, by Lemma 3.3(a), we have $W_{21} = W_{96} = W_{23}$ and the cycle again collapses.

$m = 89$: Here $\sigma = (1\,11\,39\,25)(3\,43\,23\,33\,7\,41)(5\,21\,17\,9)(13\,19\,35\,27\,31\,29\,15\,37)$, so we check $i = 3$ which is covered by Lemma 3.2, 5 and 15. For $i = 5$, by Lemma 3.3(b), we have $W_{-1} = W_{24} = W_{-65}$, so the cycle collapses and for $i = 15$, by Lemma 3.3(a), we have $W_{22} = W_{112} = W_{23}$ and the cycle again collapses.

$m = 97$: Here $\sigma = (1\,3\,47\,25\,9\,11\,43\,27\,35\,31\,33)(5\,23\,37\,15\,41\,7\,45\,13\,21\,19\,39\,29\,17)$, so this time we check only $i = 5$. For $i = 5$, by Lemma 3.3(b), we have $W_{-9} = W_{56} = W_{-41}$, so the cycle collapses.

$m = 109$: Here $\sigma = (1\,27\,41\,17\,23\,43\,33\,19\,45)(3\,53\,7\,51\,29\,5\,13)(9\,25\,21\,11\,49\,15\,47\,31\,39\,35\,37)$, so we check $i = 3$ which is covered by Lemma 3.2, and 9. For $i = 9$, by Lemma 3.3(a), we have $W_3 = W_{80} = W_{-29}$, so the cycle collapses.

$m = 113$: Here $\sigma = (1\,7\,53\,15\,49)(3\,55\,29\,23\,45\,17)(5\,27\,43\,35\,39\,37\,19\,47\,33)(9\,13\,25\,11\,51\,31\,41)$, so we check $i = 3$ which is covered by Lemma 3.2, 5 and 9. For $i = 5$, by Lemma 3.3(b), we have $W_{-17} = W_{88} = W_{-25}$, so the cycle collapses and for $i = 9$, by Lemma 3.3(a), we have $W_{-1} = W_{80} = W_{33}$ and the cycle again collapses.

The choice of 127 as a stopping point in (a) was far from arbitrary, as this technique fails there — for 127, σ has a cycle (11 29 49 39) which contains no numbers of the form $2^k \pm 1$. It is perhaps not surprising that a Mersenne prime causes problems, as the order of 2 is very low in such cases. The next Fermat prime, 257, also poses a problem, as for it σ has a cycle (11 123 67 95 81), which again has no numbers of the form $2^k \pm 1$.

References

[1] D.E. Bryant, Varieties of quasigroups and related topics, Ph.D. Thesis, The University of Queensland, Queensland, 1992.

[2] D.E. Bryant and C.C. Lindner, 2-perfect m-cycle systems can be equationally defined for $m = 3$, 5 and 7 only, Algebra Universalis 35 (1996) 1–7.

[3] D.E. Bryant and S. Oates-Williams, Constructing identities for finite quasigroups, Comm. Algebra 22 (1994) 1783–1795.

[4] A.D. Keedwell, Some connections between latin squares and graphs, Atti dei Convegni Lincei 17, Colloquio Internationale sulle Theorie Combinatorie, Roma, 3–15 settembre 1973 (Accademia Nationale dei Lincei, Roma, 1976) 321–329.

[5] A.D. Keedwell, Decompositions of complete graphs defined by quasigroups, Ann. Discrete Math. 12 (1982) 185–192.

[6] A. Kotzig, Groupoids and partitions of complete graphs, in: Combinatorial Structures and their Applications, Proc. Calgary Internat. Conf. Calgary, Alta, 1969 (Gordon and Breach, New York, 1970) 215–221.

[7] C.C. Lindner, Graph decompositions and quasigroup identities, in: Proc. Second Internat. Catania Combinatorial Conf., Graphs, designs and combinatorial geometries (Universita di Catania Catania, Sicily, 4–9 September 1989). Le Matematiche XLV (1990) 83–118.

[8] C.C. Lindner and C.A. Rodger, Decomposition into cycles II, in: J.H. Dinitz and D.R. Stinson, eds., Cycle Systems in Contemporary Design Theory: A Collection of Surveys (Wiley, New York, 1992) 325–369.